The malicious use of information and communications technology (ICTs) has become one of the greatest transnational threats of today. Cyber threats are not restricted to a country’s geographical boundaries: it is possible to launch an attack in one country, but route it through another. Diplomacy is a critical tool for responding to these threats as it can foster cooperation and can help avoid misunderstandings between states.

For over a decade, the Organization of American States (OAS) has been working to promote effective cyber security policy among its membership. In 2004, OAS Member States unanimously adopted the Comprehensive Inter-American Cyber Security Strategy, which provided an official mandate under which the OAS General Secretariat (OAS/GS) could support the development of cyber security capabilities in Member States. Although there are clear differences between the capabilities of OAS Member States, the region was able to reach a consensus on the need for a comprehensive approach much earlier than other regions, demonstrating a willingness of countries to build a cohesive political platform regarding cyber security. Nevertheless, there is still much to be done, and fostering open dialogue among Member States and with the wider international community is a first step.

With this in mind, the OAS/GS and the Zurich-based ICT4Peace Foundation joined efforts to organize a workshop entitled “International Security and Diplomacy in Cyberspace.” The workshop was held in Bogota, Colombia, from November 18-20, 2014, and was attended by participants from some 26 Member States and several international organizations from across the diplomatic, defense, law enforcement and technical communities.

Designed with the support of the Ministry of Information and Communication Technologies (MinTIC) of Colombia and the governments of the United States, United Kingdom and Canada, the workshop aimed to provide a clear explanation and understanding for cyber policymakers and diplomats in the Americas of the range of international and regional cyber security
processes currently underway, including those pertaining to norms and confidence building measures (CBMs) taking place within the framework of the United Nations Group of Governmental Experts (GGE), the UN General Assembly’s First Committee on Disarmament, the Organization for Security and Cooperation in Europe (OSCE) and the ASEAN Regional Forum (ARF). Discussions also covered cyber security initiatives led by the European Union, the Council of Europe, the International Telecommunications Union (ITU), the UN Office on Drugs and Crime (UNO-DC) and national and regional Computer Emergency Response Teams (CERTs, also commonly referred to as CSIRTs).

The first day of the event provided attendees a general background of cyber security at the international level, encompassing matters of international law and the important role international/regional organizations can play in building a common understanding among states. On the second day, attendees were assigned to five groups for a negotiation simulation exercise to practice and apply key cyber security themes discussed during the first day. The aim of the exercise was to have Member States’ representatives propose a cyber security confidence-building measure (CBM) and try to arrive at a consensus in favor of one or more such measure. During the last day of the event, Member States had the opportunity to discuss the
The Internet is everywhere, connecting people's daily relations and transactions no matter their geographic location.

different perspectives on the cyber space and to learn about the Colombian experience in tackling cyber security threats. This report provides a summary of the three-day event. The first section focuses on the importance of diplomacy in responding to the malicious use of ICTs, including ongoing processes aimed at reaching consensus on norms for responsible state behavior and CBMs in cyberspace. The second section provides insight into the different perspectives that could be considered when addressing cyber security policies, such as international, industrial, policy, and technical perspectives. The third and final section describes the main takeaways and potential policy options for the region. An overview of the status of cyber security policy in Colombia is provided at the end of this report.
The Internet is everywhere, connecting people’s daily relations and transactions no matter their geographic location. Notwithstanding the lack of physical borders in cyberspace, the reality is that network infrastructure is physically located within a state’s jurisdiction and therefore subject to a state’s legislation. In other words, despite the perceived borderless nature of cyberspace, it strongly relies on physical infrastructure owned and operated by companies, which are incorporated in a sovereign state. Therefore diplomacy plays an important role in the definition of a strategy to address cyber threats, particularly general principles and values to guide countries’ behavior towards conflicts involving cyber space. Defining general principles for countries’ behavior at the international level not only upholds fundamental values of freedom and privacy, but also facilitates global interoperability and network stability.

For more than a decade, OAS Member States have been working to build consensus on cyber security matters. In 2004, the OAS General Assembly unanimously adopted the Comprehensive Inter American Cyber Security Strategy, which recognized the need for multi-stakeholder engagement. In 2012, the governments of the Americas signed a declaration on Strengthening Cyber Security in the Americas, in which they expressed concern about growing cyber security threats, while reiterating their ongoing support to the premises of the cyber security strategy previously adopted. In comparison, the European Union only approved a comprehensive cyber security strategy in 2013. Nevertheless, despite the OAS’ early policy work in this area, much remains to be done across the Americas.

During the first day of the workshop, panelists and Member States representatives shared views on how these challenges could be addressed. Participants agreed that, to respond to cyber threats and deal with challenges of attribution, greater exchange of information between...
It is essential that governments provide guidance on how technical experts and diplomats can deal with cyber security issues at the international level.

Neil Klopfenstein, Executive Secretary of the Inter-American Committee against Terrorism (CICTE), Organization of American States (OAS).
technical experts and technical response teams across countries is required. This evidently involves some level of international cooperation, making diplomacy an essential part of cyber security policies. However, technical experts do not necessarily know how to transfer their needs to the diplomatic debate on the one hand, and diplomats have limited technical understanding of fundamental cyber security issues on the other. In order to ensure effective international cooperation for sharing information, discussions at the international level must therefore incorporate perspectives of both technical and diplomatic groups to mitigate the effects of oversights on both fronts.

But first, it is essential that governments provide guidance on how technical experts and diplomats can deal with cyber security issues at the international level. Regarding cybercrime, it was suggested that states consider joining the Council of Europe’s Convention on Cybercrime (also known as the Budapest Convention), which provides a baseline for responding to specific crimes and for exchanges of information. The G8 24/7 Network of Contact Points is also a useful mechanism, ensuring speedy assistance for data preservation. Nevertheless, few countries in the Americas have requested accession to these instruments and mechanisms. An additional challenge to effective international cooperation is the lack of national consensus on cyber security. Without strong political leadership and coordination between different parts of government, cyber security incident response actions and international engagement are inhibited.

Keeping in mind that international agreements do not require the same level of specificity as national regulations, the panelists highlighted the importance of promoting a critical reflection on the international instruments applied so far in order to define which ones can be used for ensuring cyber security and stability at the international level, such as human rights, privacy, freedom of expression, and key principles of international law.
such as sovereignty. The absence of the word ‘cyber’ in a norm does not automatically prevent its application. For instance, although the UN Charter prohibition of use of force does not mention ‘cyber,’ and was agreed before the emergence of the digital era, the fundamental concern of non-use of force and the premise of self-defense are general principles with wide application. In other words, legal principles of state responsibility and sovereignty must be complied with regardless of explicitly stating their applicability to cyberspace matters. Therefore, instead of developing new legal approaches to address cyber security issues at the international level, states could work to reach a consensus on the need to achieve legal certainty in the cyberspace based on existing international legal frameworks.

Not all states face the same cyber security challenges and therefore responses should be consistent with domestic realities. At the same time, nation states that stand for certain values should come together to decide how to deal with cyber security. Cyber disruption and other malicious uses of ICTs are novel and unclear concepts, ranging from events that cause mere inconvenience to cyberattacks that can ultimately cause significant damage or injure people. For this reason, dialogue between nations to find common understandings of both challenges and possible responses is of utmost importance.

Bearing this in mind, the panelists offered a 5-step thinking structure to assist in the application of international law in the international cyber dialogue. First, states should define the jointly desired and undesired outcomes. In general, countries agree on the development of an open, resilient, stable, secure and peaceful cyberspace, where economic transactions and social interactions are encouraged and not overshadowed by security threats. The debate over these general principles should be the starting point for reaching consensus on the application of international law. Once the outcomes are defined, states should come together to
analyze current international norms and identify whether there are gaps in the existing international legal framework. The third step refers to how countries could deal with existing gaps. For some cases, the existing legal framework could be differently construed in order to encompass cyber issues. If this is not possible, states can move to the next step, which would consist in taking substantive action, such as soft regulation rather than treaties. The former is preferred given the incipient stage of international dialogue on cyber security matters. To put in another way, a soft regulation allows countries to tackle this matter in a flexible way without making far-reaching conclusions and setting prescriptive norms that could limit future generations’ work. Finally, states could identify norms and practices that are already in place, particularly norms that emerged from cooperation among CERTs when dealing with real threats.
Confidence Building Measures (CBM) are also an interesting instrument of international politics, which is being employed to strengthen international peace and security in the cyberspace. As outlined by the 2013 report of the UN Group of Governmental Experts on “Developments in the Field of Information and Telecommunications in the Context of International Security” (A68/98*), international and regional organizations play an important role in the implementation of CBMs among their Member States. For instance, in order to reduce the risks of conflict stemming from the use of information and communications technology, participating States of the OSCE agreed in December 2013 on a first set of CBMs designed to enhance interstate cooperation, transparency, and predictability in the cyberspace. (a) The gist of these measures was to diminish and eliminate potential causes of misunderstandings between states that could lead to conflict in the absence of absolute certainty.

An interesting aspect of OSCE CBMs is that they mainly target policymakers including those responsible for foreign policy who are likely to play an important role on how to respond to a malicious cyber action believed to originate from another state. The OSCE CBMs can broadly be put into three clusters: 1. CBMs that involve the provision of specific information to other states (e.g., national cyber security strategies); 2. CBMs that encourage states to communicate or to meet, including to defuse the emergence of tensions; and 3. CBMs that encourage putting in place steps and frameworks which facilitate coordination on the national and international level to deal with cyber threats.

Most generally, the elaboration and implementation of CBMs represent an opportunity for countries to show partners the importance a state attaches to stability between countries through increased levels of transparency and predictability.

Understanding the industry’s perspectives on cyber security and working with the sector can help nation states not only to increase their knowledge about their cyber status, but also to improve their incident response capacity towards cyber threats. Given their large customer bases, companies have access to real-time information on cyber threats and can provide valuable insight into the latest techniques being employed against OAS Member States. For example, the OAS/GS recently partnered with Symantec to produce a comprehensive report on cyber security trends in Latin America and the Caribbean.

By combining efforts with Symantec, the OAS/GS was able to better understand the type of cyber security threats and risks that states and citizens across the region face on a daily basis. It also highlighted states’ capacity to respond. The report revealed the importance of raising awareness among citizens in order to better equip Internet end-users with essential security skills to protect themselves from cyber threats. Data from 2013 revealed how Internet users’ behavior on mobile devices is risky in Latin America and the Caribbean: 50 percent of mobile users do not use basic security precautions, such as passwords, security software or backup files for their mobile device. Social networking sites represent a potential target for cybercriminals, considering that almost 95 percent of Internet users in the region actively use these sites, and that countries in the region occupy five of the top ten spots globally for the most time spent on social networks. The report also identified the great use of spear-phishing emails for the purpose of targeted attacks.

Cyber criminals often seek access to sensitive information from governments, private enterprises, and users’ banking information. Several attacks have targeted countries’ critical infras-

Through a collective approach towards cyber security, countries could build a framework of forward-looking principles aimed at paving the way for the peaceful and transparent use of cyberspace and ICTs.
tructure (e.g., oil, electricity, and water supply), in order to disrupt the provision of basic services and affect governments’ credibility towards their constituents.

Today private enterprises are developing several goods and services connected to the Internet (i.e. the so-called Internet of Things), in which objects of people’s daily life will have digital sensors, connecting the physical and digital worlds in an unprecedented fashion. Additionally, Internet infrastructure is mostly owned and operated by the private sector. Despite the industry’s increasing reliance on ICTs to conduct business and provide essential services, cyber security has not been a top priority for private companies. It is therefore important that governments work together with the private sector as well as consider its perspective about cyber issues, recognizing that cyber security is a shared responsibility.

For example, the Government of Colombia has been working with Microsoft in order to align goals and better understand cyber security challenges and risks in the country. Together they identified important quantitative information regarding cyber trends, including the fact that 52 percent of Colombians used pirate software in 2013. (c) This sort of data allows governments and the private sector to better allocate resources and formulate more effective policies.

In addition to understanding the private sector’s perspective about cyber security at national level, it is important that countries be prepared to consider other nations’ perspective as well. Through a collective approach towards cyber security, countries could build a framework of forward-looking principles aimed at paving the way for the peaceful and transparent use of cyberspace and ICTs. Panelists described some examples of agreements reached at the

Cyber security is only going to grow in importance as an issue of international security and diplomacy.
international level that enhance cooperation and communication between countries in the case of cyber incidents. For example, in 2013, a United Nations Group of Governmental Experts (GGE) agreed on a substantial report entitled “Developments in the Field of Information and Telecommunications in the Context of International Security” (d), which presented a set of specific measures for the purpose of increasing transparency and establishing communication mechanisms to mitigate potential misunderstanding between nations. In addition, the report acknowledged the applicability of norms derived from existing international law to state behavior in cyberspace, while also highlighting the need to focus on capacity building and to elaborate confidence-building measures. The latter could be an important step to increase transparency, predictability, and cooperation among nation states. The report also stressed the importance of engaging the private sector, civil society and academia on these issues.

The bilateral agreement between the United States and Russia is another important example of efforts aimed at strengthening information exchange

and preventing international conflict. In June 2013 during the G8 Summit in Northern Ireland, US President Barack Obama and Russian President Vladimir Putin jointly announced a bilateral accord on confidence-building measures in the cyber domain, which included information sharing between their national CERTs, expansion of the nuclear hotline to provide direct communication during cyber crisis, and establishment of a cyber security working group within the framework of the US-Russia Bilateral Presidential Commission. This bilateral agreement reinforces the reality that cyber security must become a top priority for all countries, and only through joint work will nation states be able to tackle wrongful acts in cyberspace and avoid the escalation of tensions.

Discussions emphasized the need for policy and technical perspectives to be taken into account by nation states. In general, the implementation of cyber security policies requires a great deal of lawmaking either to adapt current legislation to digital trends or to adjust a country’s legislation to international conventions. To these ends, it is critical to employ a multi-stakeholder approach, in which all relevant ac-
tors are somehow engaged in the decision-making process. Cyber security is a relatively new concept, in which there is no consensus on basic principles and definitions, thereby demanding caution from policymakers when formulating new policies to tackle cyber threats. Otherwise, the treatment could be worse than the disease.

From the technical and operational side, the adoption of security standards and best practices are essential to protect a country’s infrastructure from cyber attacks. By partnering with the private sector, governments can have access to cyber threat intelligence tools and standards, as well as cyber security training and certification. For instance, governments could consider greater engagement with industry organizations, such as the Anti-Phishing Working Group (APWG), the Message Anti-Abuse Working Group (MAAWG) and the London Action Plan (LAP), which are geared towards the need to mitigate cyber attacks. Finally, the improvement of countries’ technical incident response capacity strongly relies on information exchanged on incidents and response techniques between national CERTs. Information sharing mechanisms that allow access to timely and accurate data about threat and actors in virtually any country, as well as to experts depending on the type of cyber threat, are vital to build a secure and reliable network. Hence diplomatic tools to establish contact points are essential for the improvement of countries’ technical response capabilities.
Attendees were then assigned to five groups for a negotiation simulation exercise to practice and apply key cyber security themes discussed during the first day. The idea of the exercise was to have Member States’ representatives propose a cyber security confidence-building measure and try to arrive at a consensus in favor of one or more such measure.

Group 1 discussed the importance of defining clear goals with the support of the OAS in such a task. In addition to considering joining the Council of Europe’s Cybercrime Convention, the group suggested that Member States work together to develop regional cyber security instruments geared towards establishing short and long-term goals for the improvement of cyber security capabilities in the region. Likewise, the second group deliberated over the creation of a working group specialized in cyber security issues in Latin America and the Caribbean. More specifically, this cyber security working group would first conduct a situational analysis of the countries’ cyber security status, and then define policies based on two axes of work: national and international. The former would be responsible for identifying relevant stakeholders, assessing countries’ legislative framework, and listing cyber incidents, while the latter would conduct an analysis of the Council of Europe’s Cybercrime Convention for potential adhesion of OAS Member States, as well as promote an annual conference on cyber security.

Other groups focused on specific measures that could be considered in any compromise on cyber security in the Americas. For example, Group 3 suggested the creation of a collaborative protocol for the exchange of information and best practices. Similarly, Group 4 stated that such collaborative platform could establish technical guidelines and lines of action for Member States to respond to cyber incidents. The standardization of incident response procedures by Member States would facilitate quantitative
Group 5 stressed the need to engage other stakeholders, especially civil society, in the fight against cybercrime. Internet users are the most vulnerable stakeholders, hence the importance that Member States promote educational programs on basic security protocols.

The Group also suggested that Member States recognize October as the “Cyber Security Awareness Month” and coordinate initiatives for public awareness throughout the region.

Attendees also discussed other measures that could be undertaken to fight cybercrime in Latin America and the Caribbean. In this regard, they tabled three main takeaways aimed at improving cy-
ber security policies in the region: Member States’ responsibility in raising cyber security awareness; Member States’ commitment towards an international debate over cyber security; and the critical role of nonprofits and international organizations in assisting countries.

Responsibility for a secure cyberspace should be shared among different stakeholders, thereby requiring strong commitment from Member States to raise awareness of cyber security matters. To help Member States in this task, the OAS has partnered with STOP.THINK.CONNECT, a global cyber security awareness raising initiative focused on improving collaborative cyber security efforts among countries in the Americas. This partnership aims to assist Member States in the design of cyber awareness raising programs based on the needs of specific stakeholder groups. Member States could also join the Anti-Phishing Working Group (APWG), which unifies efforts to fight cybercrime, proving members the opportunity to discuss phishing and to access resources for cyber security applications.

For a fruitful international commitment, a coherent national position regarding cyber security is critical. Having a clear idea of how they desire to conduct short and long-term cyber security policies will help countries ensure that their interests are considered at international level; otherwise, countries may end up accepting what other countries have decided without a stronger voice in cyber matters. Nation states must seek an effective role in international cyber security policy. However, they also have to keep in mind the need to focus on international elements when negotiating international commitments rather than on domestic cyber security issues. To put it another way, nation states should concentrate their efforts on outcomes that are comparable at the global level. Nonprofits and international/regional organizations can play an important role in assisting countries in this task to achieve an open, secure and resilient cy-
Cyberspace at the global level. Nonprofit organizations, such as the ICT4Peace Foundation, work on fostering the exchange of best practices and contribute to the establishment of broad principles through working groups and workshops. Likewise, international and regional organizations can help countries develop their cyber security capabilities through a number of actions. For instance, along with the Inter-American Development Bank (IDB), the OAS/GS has initiated a study aimed at deepening understanding of the cyber security risks and challenges in Latin America and the Caribbean in order to better support countries’ efforts to respond.

The OAS/GS has also been developing a hemispheric network of CSIRTs, which aims to work as a contact point and information sharing mechanisms between CSIRTs from Member States. This platform will allow Member States assist each other in incident response processes. Hence international and regional organizations can play an important role in creating platforms that enable states to formulate and implement cohesive cyber security policies.
On the last day of the event, participants had the opportunity to learn about the Colombian experience regarding cyber security policies. The Colombian case is noteworthy given that in 2011, Colombia was the first country in the hemisphere aside from the US and Canada to officially adopt a comprehensive National Cyber Security Strategy. The session comprised high-level authorities from the National Police, the Ministry of Defense, as well as from the Ministry of Information Communication and Technologies (MinTIC), in order to provide attendees a wide-ranging understanding of the current cyber security policies taking place in the country.

The National Police of Colombia discussed the importance of cyber forensics skills for the analysis and preservation of digital evidence for the eventual prosecution of a cyber incident. By adopting digital forensics techniques, authorities can determine the nature and source of the incident, and identify the individuals responsible for it. For instance, the National Police has implemented a malware analysis lab, as well as a platform to conduct Big Data analysis and correlation. The National Police also described some projects adopted in Colombia, stressing the importance of focusing on protecting citizens, for example, through the prevention of child pornography and other offenses on the Internet. The latter was the first police initiative of this kind in Latin America.

The Ministry of Defense discussed the importance of information sharing mechanisms to properly secure the country’s strategic and economic assets, particularly critical infrastructures. The Ministry of Defense has been implementing policies focused on cyber security based on three main levels of action. The first is the strategic level, consisting of a strong inter-sectoral collaboration and coordination with companies that own and operate critical infrastructures in the country. The second is the operational level, which defines
THE NATIONAL AND INTERNATIONAL EXPERTS SELECTED PREPARED RECOMMENDATIONS ON FOUR MAIN TOPICS: INSTITUTIONAL CAPACITIES, CYBER SECURITY CAPABILITIES, INTERNATIONAL AND MULTI-STAKEHOLDER COOPERATION, AND CYBER SECURITY LEGAL FRAMEWORKS.
specific actions and measures to protect Colombia’s critical infrastructure. The third is the tactical level, which is how the country effectively protects its infrastructure. In short, the implementation of cyber security policies includes a clear definition of goals, risk analysis, as well as an impact analysis to assess the effectiveness of the cyber security measures undertaken and the eventual need for modifications.

Finally, the MinTIC focused on the recent measures taken with the support of the OAS/GS. The Government of Colombia approached the OAS/GS for support in organizing an International Commission of Experts to assess the country’s cyber security status. After an exchange of ideas among relevant actors, the national and international experts selected prepared recommendations on four main topics: institutional capacities, cyber security capabilities, international and multi-stakeholder cooperation, and cyber security legal frameworks. To further strengthen Colombian institutional capacity towards cyber security, the experts recommended the creation of a cyber security agency, where stakeholders from different sectors could get together and address this matter based on a multi-stakeholder and shared-responsibility approach. For instance, the government has created nine working groups to discuss protocols and stan-
Cyber Security Program

In order to create cyber security capabilities in Colombia, the experts recommended offering technical and management training focused on cyber security matters. For example, the Colombian government could offer scholarships and establish a professional cyber academy to train professionals. Additionally, the experts suggested the creation of technological clusters, particularly for start-ups and small business. The need of national and international cooperation was also brought to attention. At national level, Government could issue regulations to establish mandatory incident reporting for companies that operate critical infrastructure. At international level, experts recommended joining the Interpol I-24/7 system, which facilitates the expedite exchange of information related to cybercrime. Finally, the legal framework for cyber security in the country could be improved by reforming Colombian legislation in line with the Council of Europe’s Budapest Convention, by implementing measures to enable the preservation of digital evidence, and by adopting cooperation mechanisms with Internet Service Providers to assist in cybercrime matters. The Colombian experience reinforces a powerful message to OAS Member States: the importance of continuous international and regional cooperation to develop cyber security capabilities. By requesting the assistance of the OAS/GS and of international experts, Colombia has been able to advance the implementation of its National Cyber Security Strategy. Rather than be viewed as one-time effort, cyber security strategies require a dynamic and flexible approach, in which policies can be adapted to new digital trends as well as emerging cyber threats.